

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

224



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/756,346	01/08/2001	Henry Haverinen	442-010085-US (PAR)	6669
2512	7590	08/23/2004	EXAMINER	
PERMAN & GREEN 425 POST ROAD FAIRFIELD, CT 06824			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 08/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

### Application No.

09/756,346

### Applicant(s)

HAVERINEN ET AL.

### Examiner

Michael J Simitoski

### Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 08 January 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13, 15, 17-20 and 22 is/are rejected.
- 7) ☒ Claim(s) 9 and 15 is/are objected to.
- 8) ☒ Claim(s) 14, 16 and 21 are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2/20, 6/4, 6/18/01.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☒ Other: IDS 5/24/04.

**DETAILED ACTION**

1. The IDS of 2/20/01, 6/4/01, 6/18/01 & 5/26/04 were received and considered.
2. Claims 1-22 are pending.

***Election/Restrictions***

3. Restriction to one of the following inventions is required under 35 U.S.C. 121:
  - I. Claims 1-13, 15, 17-20 & 22 are directed to a communication system implementing cryptographic authentication, classified in class 380/270.
  - II. Claims 14, 16 & 21 are directed to a system employing a caller identification scheme, classified in class 455, subclass 415.
4. Inventions I and II are related as sub combinations disclosed as usable together in a single combination. The sub combinations are distinct from each other if they are shown to be separately usable. In the instant case, inventions I and II have separate utility, in that Group I has utility where a mobile node is cryptographically authenticated which can be used without Network Access Identifier (or other specialized form of participant identification); Group II has utility in identifying a particular telecommunications participant without the need for authentication of the participant. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

5. During a telephone conversation with Geza Ziegler on 7/30/04 a provisional election was made without traverse to prosecute the invention of Group 1, claims 1-13, 15, 17-20 & 22.

Art Unit: 2134

Affirmation of this election must be made by applicant in replying to this Office action. Claims 14, 16 & 21 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Applicant is advised that the reply to this requirement, to be complete, must include an election of the invention to be examined even if the requirement be traversed (37 CFR 1.143).

### ***Specification***

6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

7. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The limitation "providing a communications link ... not being a link of the telecommunications network" is not disclosed in the specification.

### ***Claim Objections***

8. Claim 9 is objected to because of the following informalities: "is sent" in line 2 of the claim should be removed. Appropriate correction is required.

9. Claim 15 is objected to because of the following informalities: "interfacing" in line 1 of the claim should be removed. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

Art Unit: 2134

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 4 & 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. Claim 4 recites the limitation "the at least one session secret" in lines 2-3 of the claim. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 12 recites the limitation "the at least one session secret" in line 3 of the claim. There is insufficient antecedent basis for this limitation in the claim.

14. Claim 12 recites the limitation "the at least one challenge" in line 3 of the claim. There is insufficient antecedent basis for this limitation in the claim.

### ***Claim Rejections - 35 USC § 103***

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 1, 3-5, 8-10, 13, 19, 20 & 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Protection in Mobile Communications" by Federrath, in view of Handbook of Applied Cryptography by Menezes et al. (Menezes).

Regarding claims 1, 3-4, 9-10, 13, 19, 20 & 22, Federrath discloses providing the mobile node/station with a mobile node identity/TMSI and a shared secret/Ki specific to the mobile node

identity/TMSI and usable by a telecommunications network/home network (Fig. 1, page 5), sending the mobile node identity/TMSI from the mobile node to the packet data network/visited network, providing the packet data network/visited network with authentication information usable by the telecommunications network/home network, the authentication information comprising a challenge/RAND and a session secret/Kc corresponding to the mobile node identity/TMSI and derivable using the challenge/RAND and the shared secret/Kc (Fig. 1, page 5), sending the challenge/RAND from the packet data network to the mobile node/station (Fig. 1, page 5), generating at the mobile node the session secret/Kc and a first response corresponding/SRES to the challenge/RAND, based on the shared secret/Ki (Fig. 1, page 5), sending the first response/SRES to the packet data network, and checking/authenticating the first response for authenticating the mobile node (Fig. 1, page 5). Federrath lacks providing the mobile node with a protection code, sending the protection code with the mobile node identity/TMSI, forming cryptographic information using at least the protection code and the session secret, sending the cryptographic information with the challenge to the mobile node/station and checking at the mobile node the validity of the cryptographic information using the challenge and the shared secret. However, Menezes teaches that random numbers can be used in challenge-response mechanisms to provide timeliness assurances and avoid certain replay and interleaving attacks (§10.3.1 (i)). Menezes teaches that nonces can be used to provide timeliness guarantees where a receiving party (network) creates a response (cryptographic information) that depends both on a secret/Kc and the challenge/nonce (protection code) (§10.3 & §10.3.1 Background). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the mobile node with a protection

code/nonce, send the protection code/nonce with the mobile node identity/TMSI, form cryptographic information/nonce verification using at least the protection code/nonce and the session secret/Kc, send the cryptographic information/nonce verification with the challenge/RAND to the mobile node/station and check at the mobile node the validity of the cryptographic information/nonce verification using the challenge/RAND and the shared secret/Ki. One of ordinary skill in the art would have been motivated to perform such a modification to distinguish one protocol instance from another and to prevent certain chosen-text attacks in challenge-response protocols, as taught by Menezes (§10.3 & §10.3.1).

Regarding claim 5, Federrath, as modified above, discloses a link not being a link of the telecommunications network (visited network) (page 5, Fig. 1).

Regarding claim 8, Federrath discloses obtaining a second response/SRES' by the telecommunications network/home network, and using the second response in the checking/(auth.result =?) the first response (page 5, Fig. 1).

17. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Federrath in view of Menezes, as applied to claim 1 above, in further view of "The Network Access Identifier" by Aboba et al. (Aboba). Federrath, as modified above, lacks forming a Network Access Identifier from the subscriber identity/TMSI as the mobile node identity. However, Aboba teaches that the network access identifier is known in the art as an identifier for a user, to be used in roaming and to assist in routing an authentication request (§2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a network access identifier as the mobile node identity by the mobile node, from the subscriber identity. One of



Art Unit: 2134

ordinary skill in the art would have been motivated to perform such a modification to assist in routing an authentication request, as taught by Aboba (page §2.1).

18. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Federrath in view of Menezes, as applied to claim 1, in further view of U.S. Patent 5,537,474 to Brown et al. (Brown). Federrath, as modified above, discloses using a Subscriber Identity Module, but lacks using it for the providing the mobile node with the mobile node identity and generating the session secret. However, Brown teaches that the mobile device in the GSM system includes a SIM, programmed with the subscriber identity and shared secret/Ki, which calculates the session secret/Kc (col. 5, line 26 – col. 6, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SIM for the providing the mobile node with the mobile node identity and generating the session secret. One of ordinary skill in the art would have been motivated to perform such a modification to conform to the GSM standard, as is well known in the art, and taught by Brown (col. 5, line 39 – col. 6, line 3).

19. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Federrath in view of Menezes, as applied to claim 1 above, in further view of “Internet Key Exchange (IKE)” by Harkins et al. (Harkins) in further view of Applied Cryptography, Second Edition by Schneier. Federrath, as modified above, lacks generating a session key for Internet Key Exchange, wherein the shared session key is based on the at least one session secret and the at least one challenge. However, Harkins teaches that Internet Key Exchange is a protocol used to establish authenticated keying material in IPSec (§1 & §2), which is authenticated using a pre-shared key (§5.4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a session key for Internet Key Exchange. One of ordinary

Art Unit: 2134

skill in the art would have been motivated to perform such a modification to use IPSec, as taught by Harkins (§1-2 & §5.4). As modified, Federrath lacks the session key being based on the session secret and at the challenge. However, Schneier teaches that a 'salt' is a random string applied to a password to make it more difficult to find using a dictionary attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to 'salt' the session secret/password with the challenge/random string. One of ordinary skill in the art would have been motivated to perform such a modification to make the session secret more difficult to find using a dictionary attack, as taught by Schneier (pages 52-53).

20. Claims 15, 17 & 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 01/41470 to Abrol et al. (Abrol). Regarding claims 15, 17 & 18, the claims are substantially equivalent to claim 1, but lack a gateway acting as an interface. However, Abrol teaches that by using a data service node/gateway that supports authentication between a mobile node and an authentication server, the benefit of providing authentication for a diverse set of mobile stations in a wireless network is gained (page 3, ¶2-3). The data service node/gateway performs authentication techniques for the mobile station; otherwise, an authentication server is accessed (page 3, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an authentication gateway/data service node to authenticate mobile stations. One of ordinary skill in the art would have been motivated to perform such a modification to provide authentication for a diverse set of mobile stations in a wireless network, as taught by Abrol (page 3, ¶2-3).

***Allowable Subject Matter***

Art Unit: 2134

21. Claim 11 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### ***Conclusion***

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

(703)746-7239 (for formal communications intended for entry)

**Or:**

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished


Art Unit: 2134

applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS

August 9, 2004



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100